[illegible]

www.huawei.com

[illegible] © 2018 [illegible]

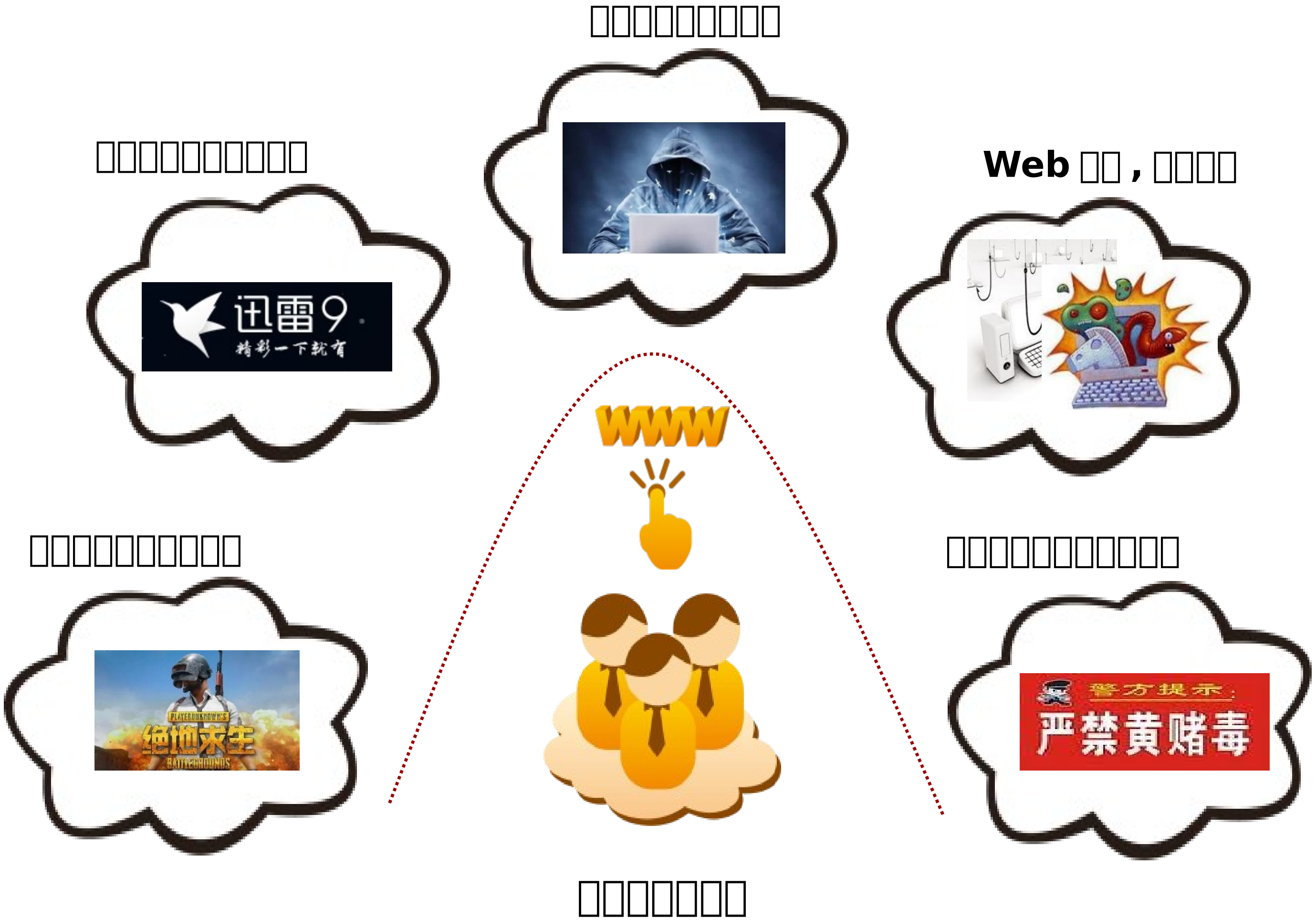
目标

- 学完本课程后，您将能够：
  - 掌握 AAA 技术
  - 掌握用户认证技术
  - 掌握用户认证管理配置

目录

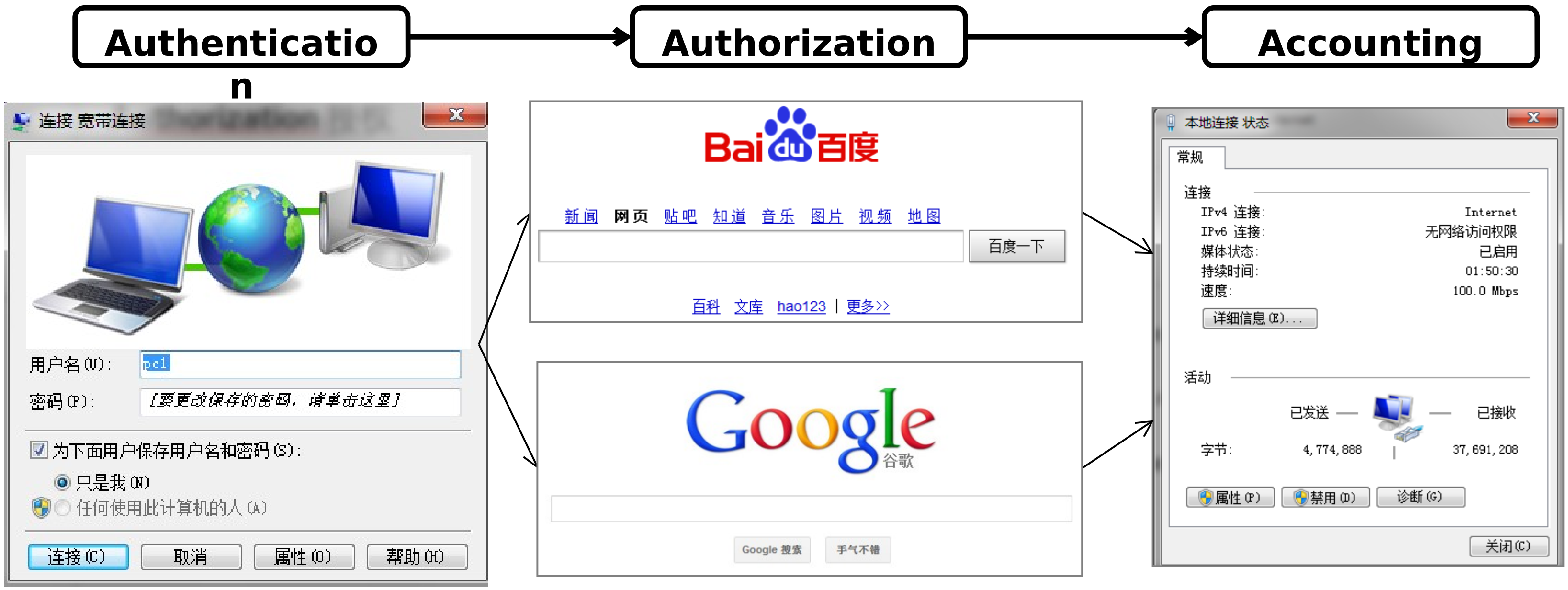
1. 用户认证和AAA技术原理
2. 用户认证管理及应用

版权所有© 2018 华为技术有限公司 第4页


Web
迅雷9
精彩一下就有
WWW
绝地求生
BATTLEGROUNDS
警方提示：
严禁黄赌毒

□□□ AAA

- Authentication □□
- Authorization □□
- Accounting □□



Authentication 认证

- 认证是指通过一定的手段，完成对用户身份的确认。
  - 你所知道的信息
  - 你所拥有的东西
  - 独一无二的身体特征

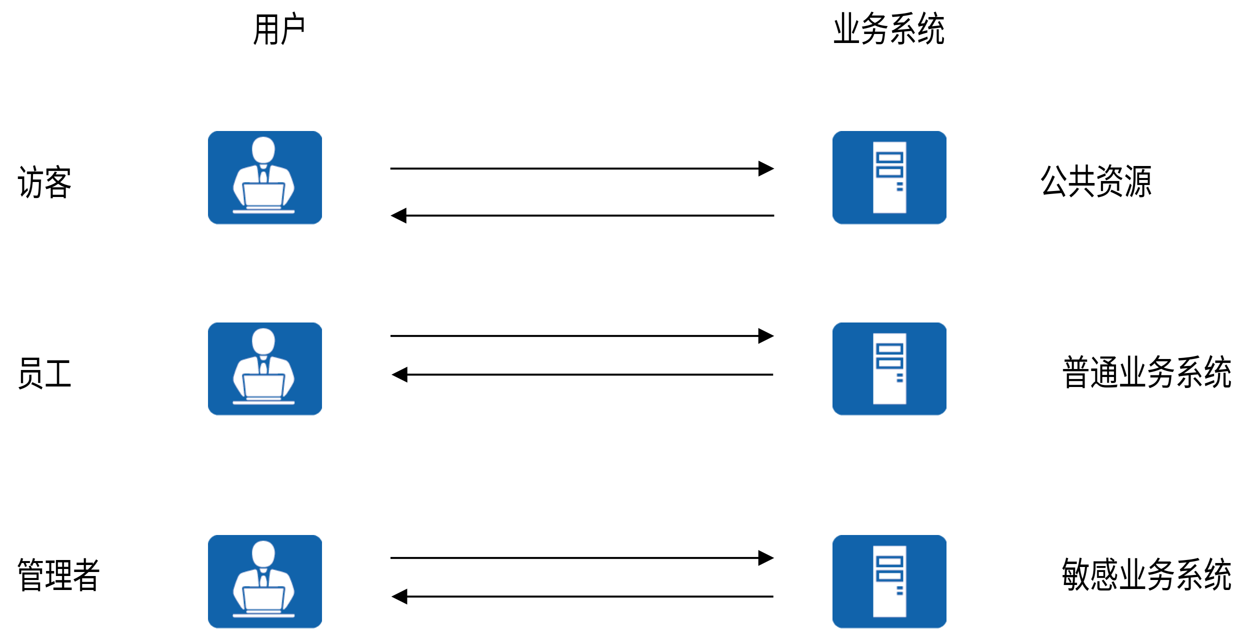
密码验证

USB 证书认证

HUAWEI

Authorization 授权

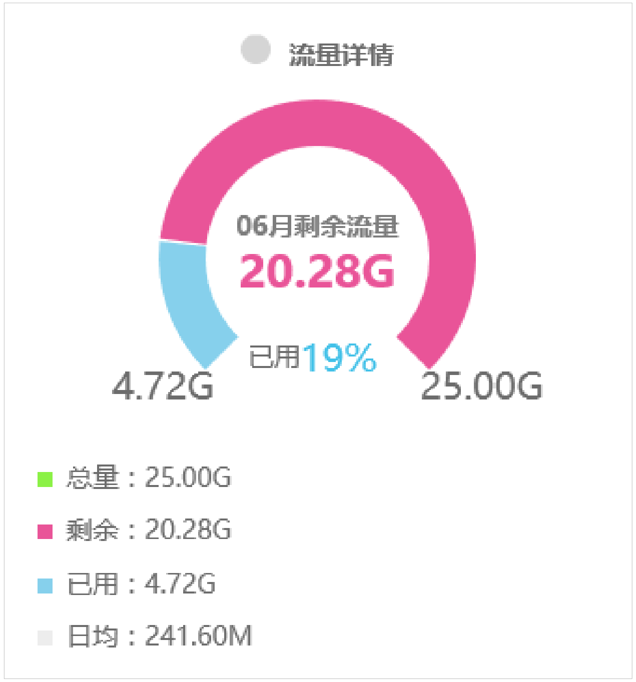
- 用户能访问的资源
- 用户能使用的命令



版权所有 © 2018 华为技术有限公司

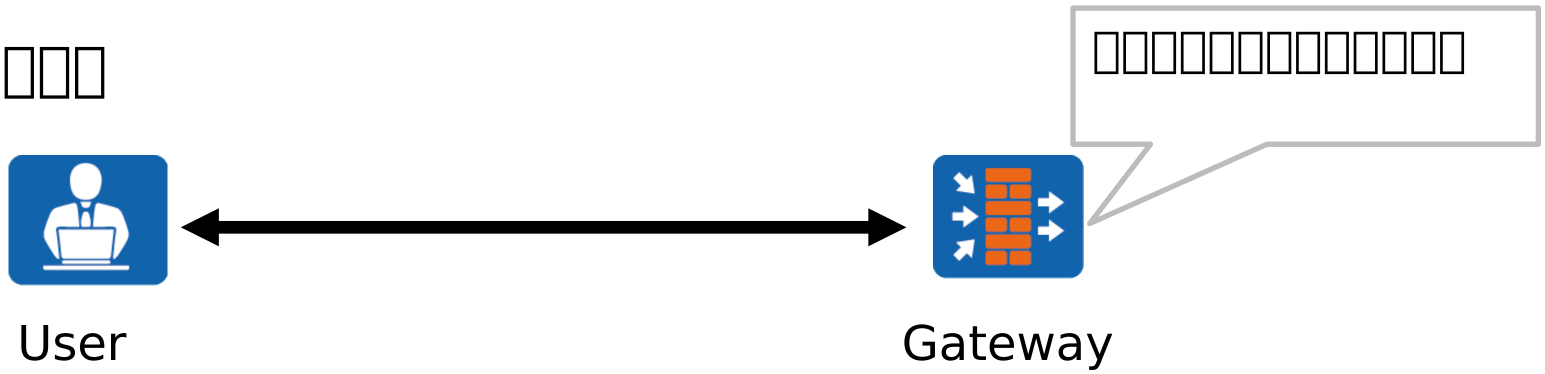
Accounting [illegible]

- [illegible]
- [illegible]
- [illegible]

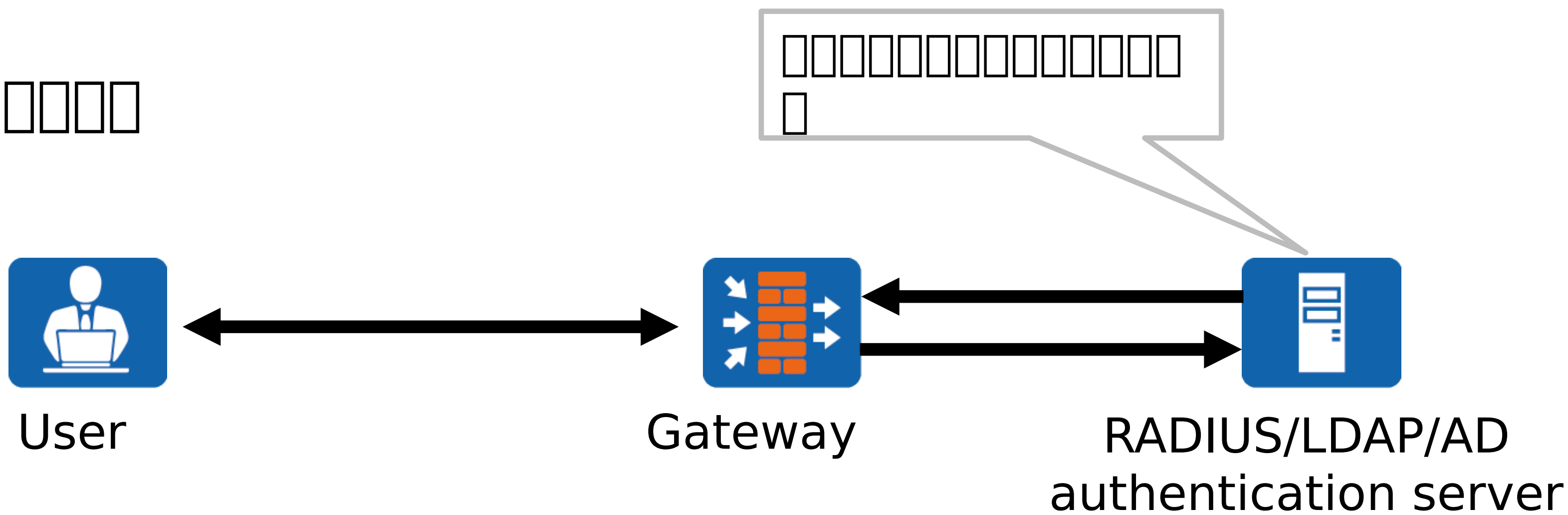

流量详情
06月剩余流量
20.28G
已用19%
4.72G
25.00G
总量：25.00G
剩余：20.28G
已用：4.72G
日均：241.60M

AAA [illegible]

- [illegible]

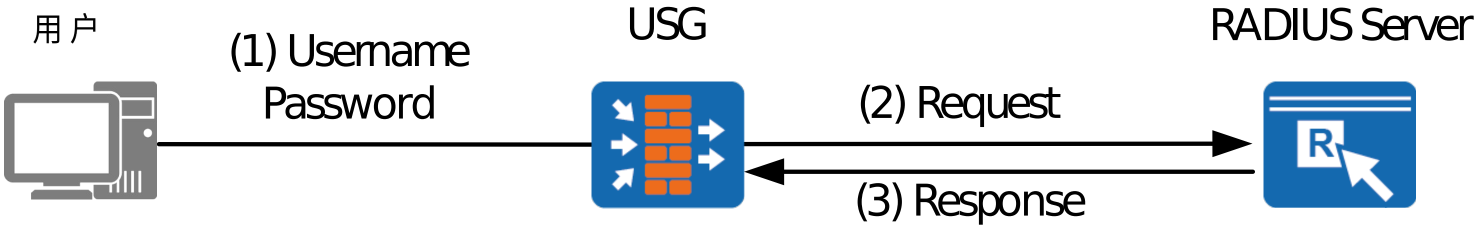

User
Gateway

- [illegible]

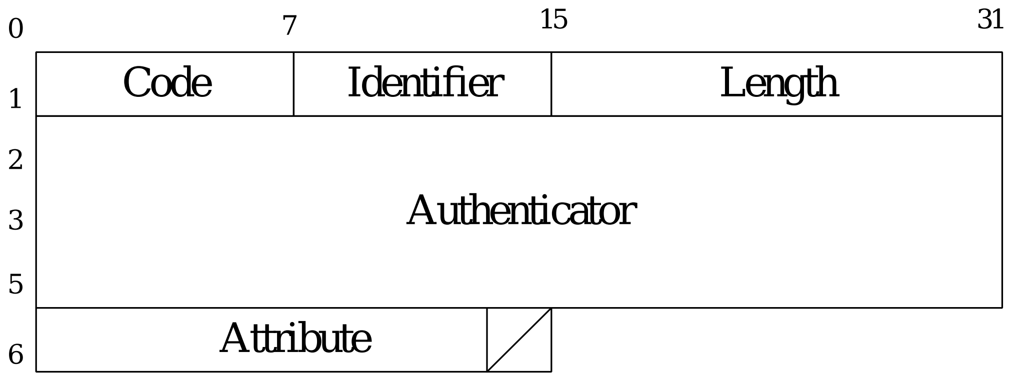

User
Gateway
RADIUS/LDAP/AD
authentication server

RADIUS 协议概述

- RADIUS 服务器通过建立一个唯一的用户数据库，存储用户名、密码来对用户进行验证。

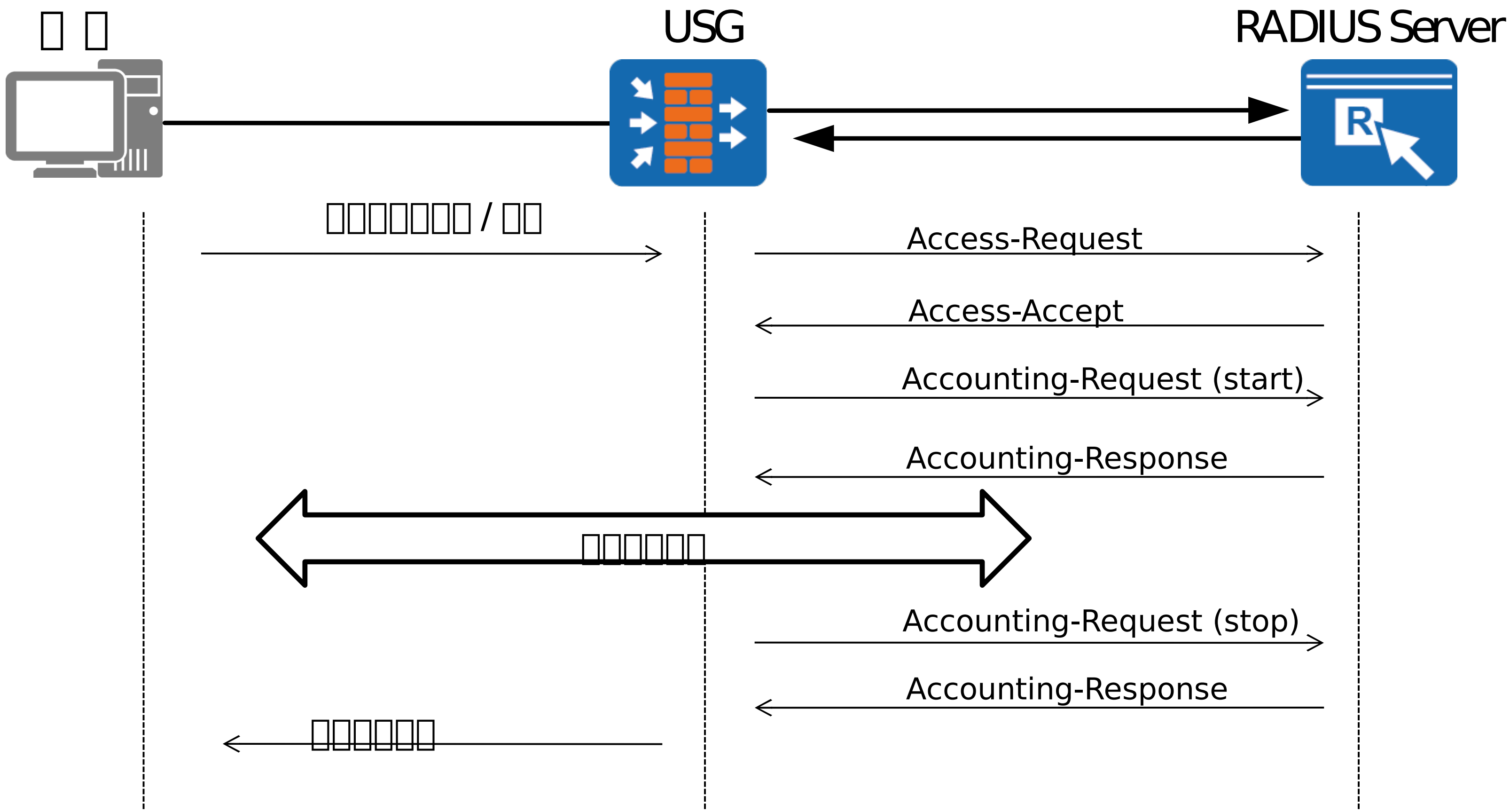


- RADIUS 的消息结构如图所示



版权所有 © 2018 华为技术有限公司

RADIUS □□□□



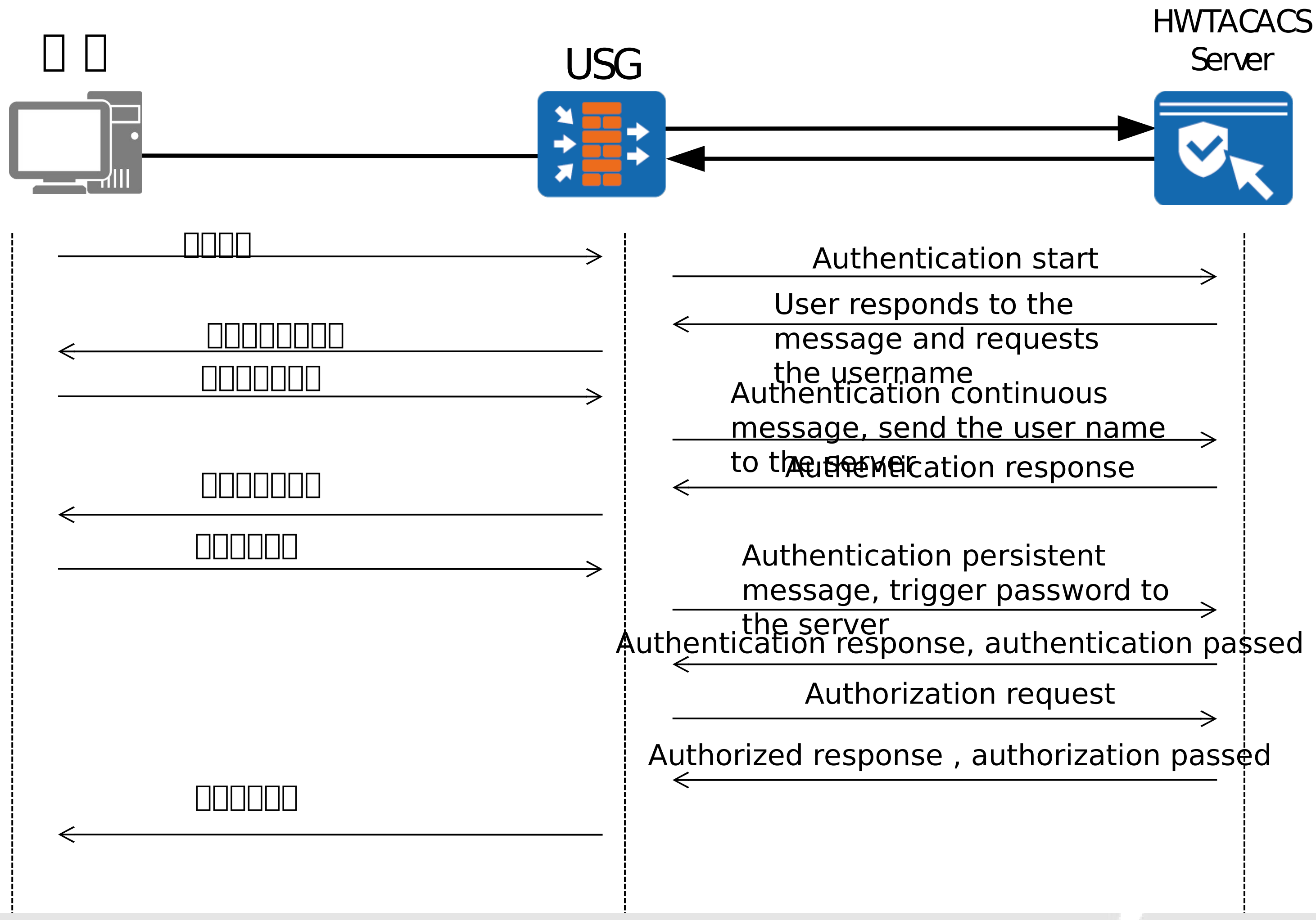
□ □
USG
RADIUS Server
□□□□□□□ / □□
Access-Request
Access-Accept
Accounting-Request (start)
Accounting-Response
□□□□□□
Accounting-Request (stop)
Accounting-Response
□□□□□□

HWTACACS协议概述

• HWTACACS是在TACACS协议的基础上进行了功能增强的安全协议。该协议与 RADIUS协议的功能类似，采用客户端/服务器模式实现 NAS与TACACS+ 服务
器之间的通信。
• HWTACACS的典型应用是对需要登录到设备上进行操作的终端用户进行认证、授权、计费。设备作为 HWTACACS的客户端，将用户名和密码发给 HWTACACS服务器进行验证。用户验证通过并得到授权之后可以登录到设备上进行操作。

版权所有© 2018 华为技术有限公司 第 13页

HWTACACS [illegible]


[illegible]
USG
HWTACACS Server
[illegible]
Authentication start
User responds to the message and requests the username
[illegible]
[illegible]
Authentication continuous message, send the user name to the server
Authentication response
[illegible]
[illegible]
Authentication persistent message, trigger password to the server
Authentication response, authentication passed
Authorization request
Authorized response , authorization passed
[illegible]

HWTACACS 和 RADIUS 比较

- HWTACACS 协议与 RADIUS 协议的比较。

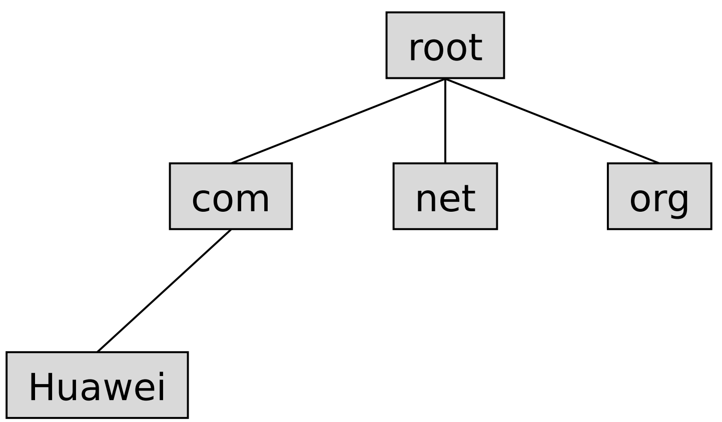
	HWTACACS	RADIUS
端口使用	使用 TCP 协议	使用 UDP 协议。认证和授权端口号是 1812 和 1813，或者 1645 和 1646
加密情况	除了标准的 HWTACACS 报文头，对报文主体全部进行加密	只是对认证报文中的密码字段进行加密
认证和授权	认证与授权分离	认证与授权一起处理
应用	适于进行安全控制	适于进行计费
配置命令授权	支持对配置命令进行授权	不支持对配置命令进行授权

版权所有 © 2018 华为技术有限公司

HUAWEI

LDAP协议概述

• LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）是从X.500目录访问协议的基础上发展过来的，X.500是层次型的，所有对象被组织成树形结构。X.500目录服务实现身份认证、访问控制。LDAP就是简化 X.500目录的复杂度，同时适应 Internet的需要。



版权所有© 2018 华为技术有限公司 第 16页

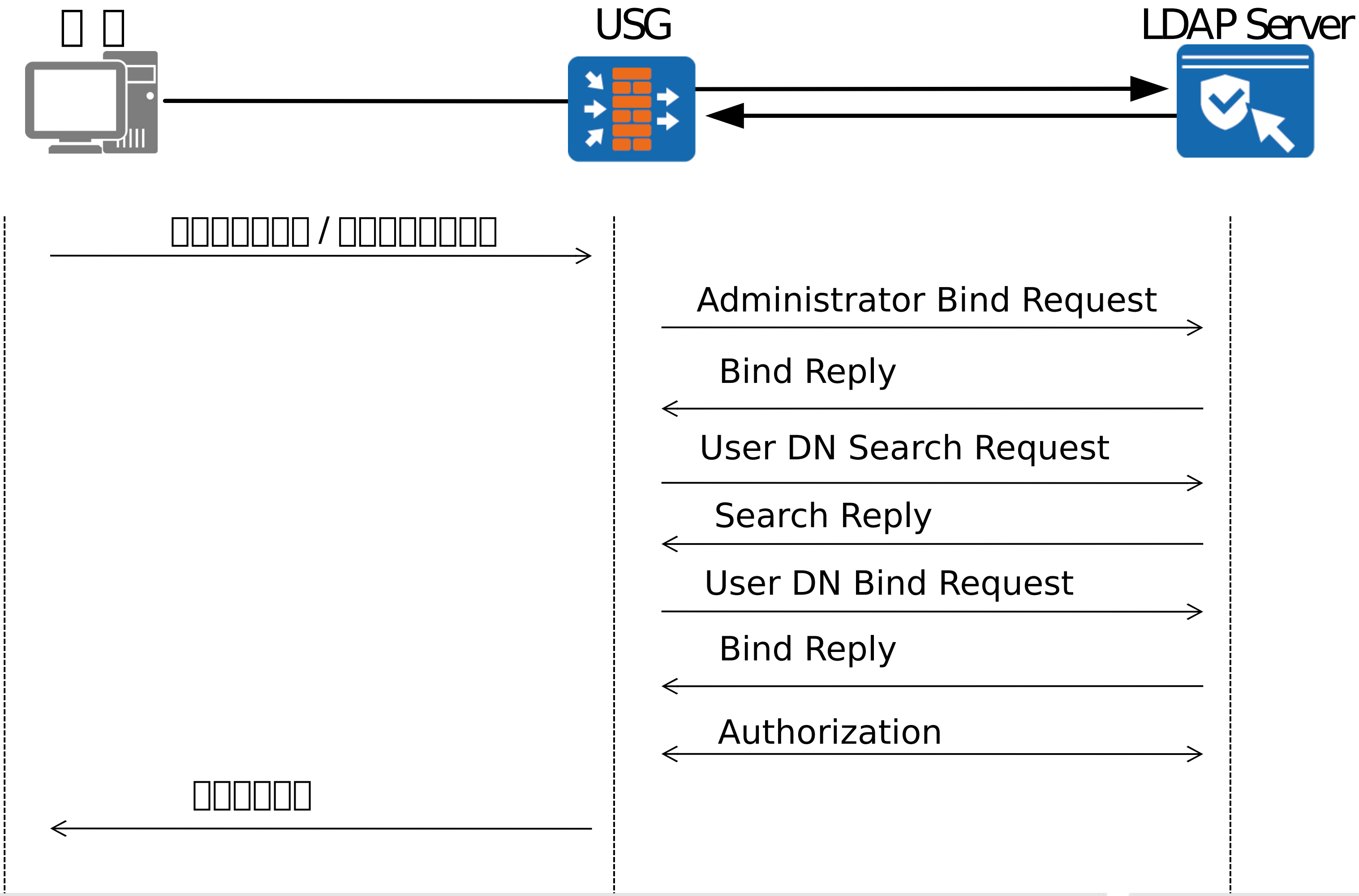
LDAP 基本概念

- 在 LDAP 中，信息以树状方式组织，基本数据单元是条目，而每个条目由属性构成，属性由类型（Type）和一个或多个值（Value）组成。
- 目录信息树 DIT （Directory Information Tree）
  - 目录条目的集合构成目录信息树。
- 条目 Entry
  - 目录信息树中的一个节点，是目录信息中最基本的单位，由一系列属性构成。
- 属性 Attribute
  - 属性描述对象的特征，一个属性有属性类型和一个或多个属性值构成。
- 相对标识名 RDN （Relative Distinguished Name）
  - 条目的名字，唯一标识同一父条目的子条目。
- 唯一标识名 DN （Distinguished Name）
  - 在一个目录信息树种唯一标识一个条目的名字。

版权所有 © 2018 华为技术有限公司

HUAWEI

LDAP [illegible]


[illegible]
USG
LDAP Server
[illegible] / [illegible]
Administrator Bind Request
Bind Reply
User DN Search Request
Search Reply
User DN Bind Request
Bind Reply
Authorization
[illegible]

[illegible] © 2018 [illegible]

用户认证分类

- AAA 技术为用户认证提供手段。
- 用户认证分类有：
  - 本地认证
  - 服务器认证
  - 单点登录
  - 短信认证

版权所有 © 2018 华为技术有限公司

HUAWEI

目录

1. 用户认证和 AAA 技术原理
2. 用户管理及应用
   - 用户组织架构及分类
   - 管理员认证流程和配置
   - 上网用户及接入用户认证流程
   - 用户认证策略
   - 上网用户认证配置

版权所有 © 2018 华为技术有限公司

HUAWEI

用户管理的背景

AAA 认证技术 → 用户认证 → 用户管理

版权所有 © 2018 华为技术有限公司

HUAWEI

用户组织架构

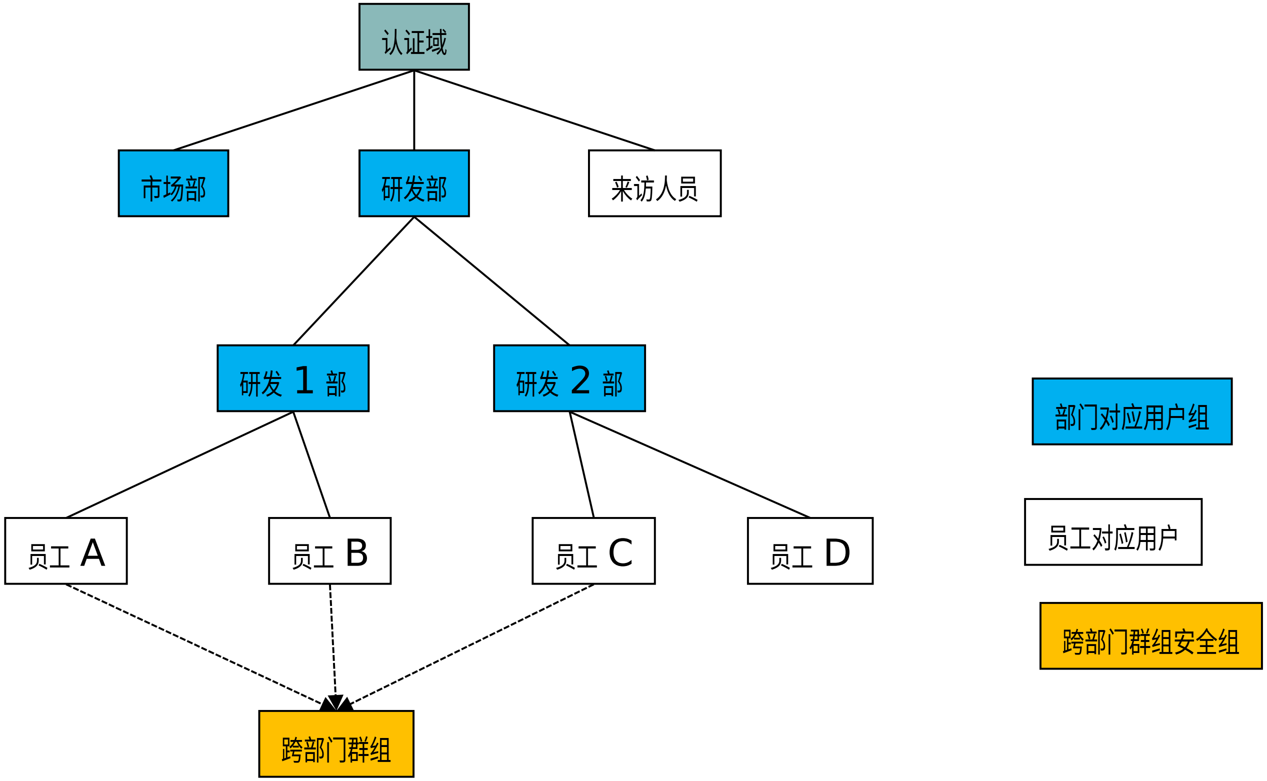
- 用户是网络访问的主体，是 FW 进行网络行为控制和网络权限分配的基本单元。
- 用户组织结构中涉及如下三个概念：
  - 认证域：用户组织结构的容器，防火墙缺省存在 default 认证域，用户可以根据需求新建认证域。
  - 用户组 / 用户：用户按树形结构组织，用户隶属于组（部门）。管理员可以根据企业的组织结构来创建部门和用户。
  - 安全组：横向组织结构的跨部门群组。当需要基于部门以外的维度对用户进行管理可以创建跨部门的安全组。例如企业中跨部门成立的群组。

版权所有 © 2018 华为技术有限公司

HUAWEI

组织结构管理

- 系统默认有一个缺省认证域，每个用户组可以包括多个用户和用户组。
- 每个用户组只能属于一个父用户组，每个用户至少属于一个用户组，也可以属于多个用户组。



用户分类

- 管理员
  - 管理员用户指通过 Telnet 、SSH 、web 、FTP 等协议或通过 Console 接口访问设备并对设备进行配置或操作的用户。
- 上网用户
  - 内部网络中访问网络资源的主体，如企业总部的内部员工。上网用户可以直接通过防火墙访问网络资源。
- 接入用户
  - 外部网络中访问网络资源的主体，如企业的分支机构员工和出差员工。接入用户需要先通过 SSL VPN 、L2TP VPN 、IPSec VPN 或 PPPoE 方式接入到防火墙，然后才能访问企业总部的网络资源。

版权所有 © 2018 华为技术有限公司

HUAWEI

目录

1. 用户认证和 AAA 技术原理

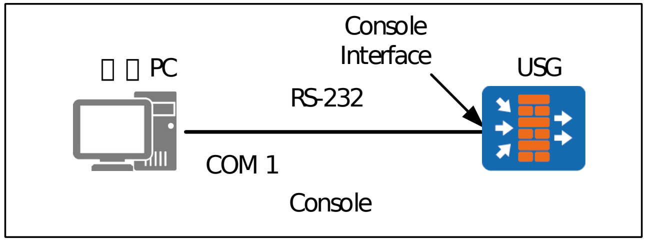
2. 用户认证管理及应用

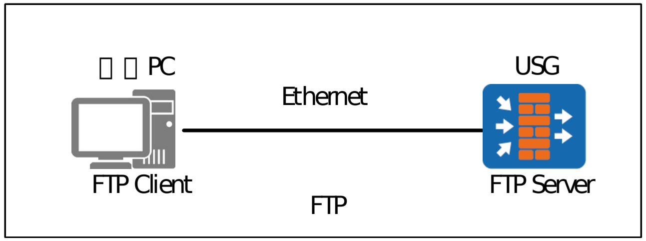
- 用户组织架构及分类
- 管理员认证流程和配置
- 上网用户及接入用户认证流程
- 用户认证策略
- 上网用户及接入用户认证配置

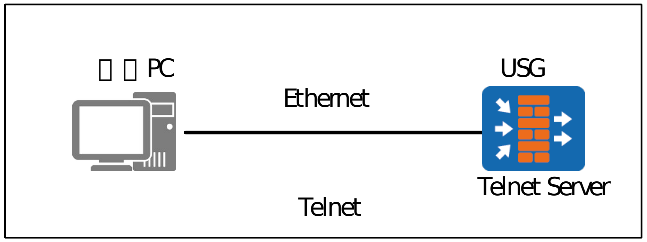
版权所有 © 2018 华为技术有限公司

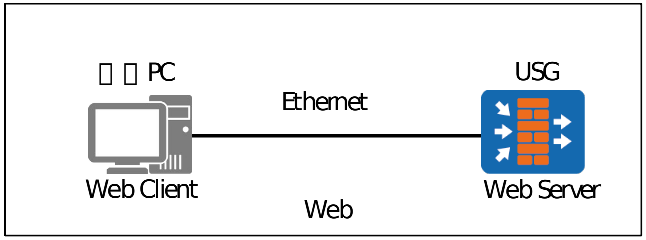
□□□□□□□

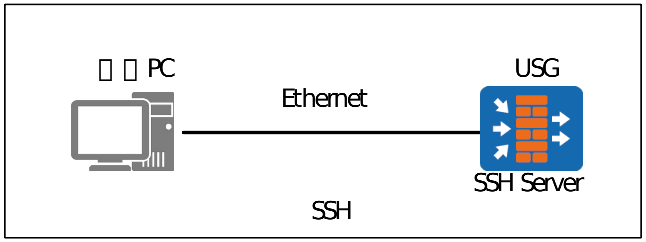
- Console
- Telnet
- SSH
- FTP
- Web









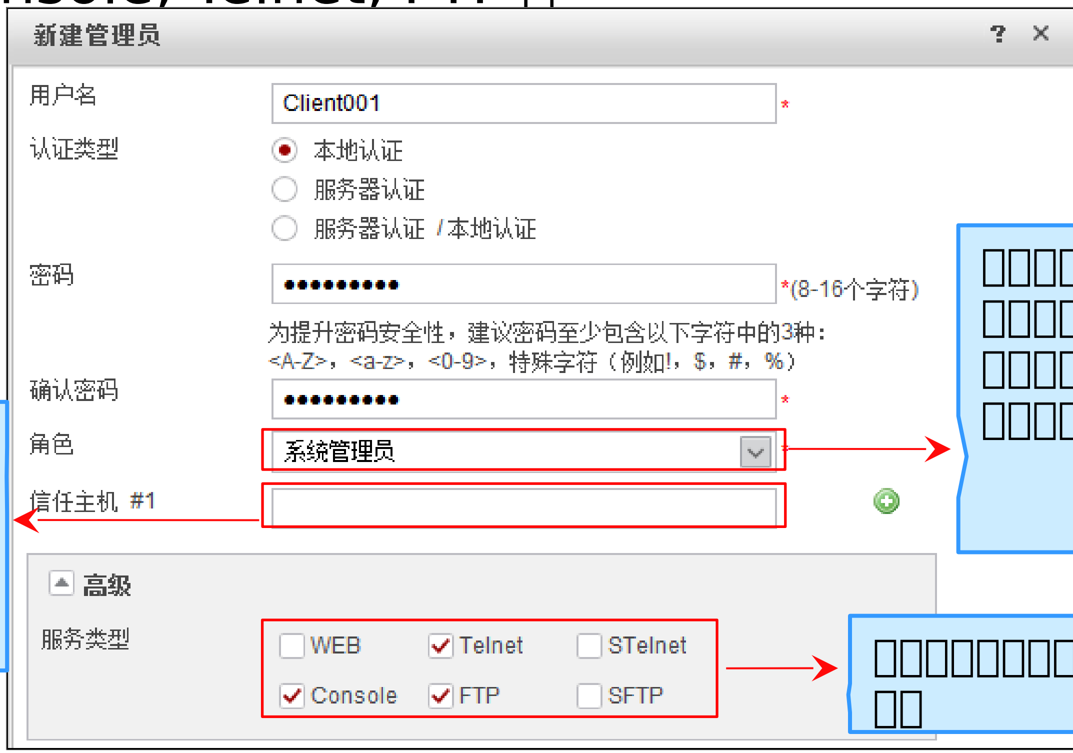


Console/telnet/Ftp设备管理类型

• 在“系统 > 管理员 > 管理员 > 新建”，新建管理员Client01，并设置设备管理类型Console, Telnet, FTP。

可为管理员选择配置不
同的角色，包含系统管
理员、配置管理员、审
计管理员。
设置信任主机
IP，指定特
定的主机访
问。
选择配置设备管理类
型。

版权所有© 2018 华为技术有限公司 第27页



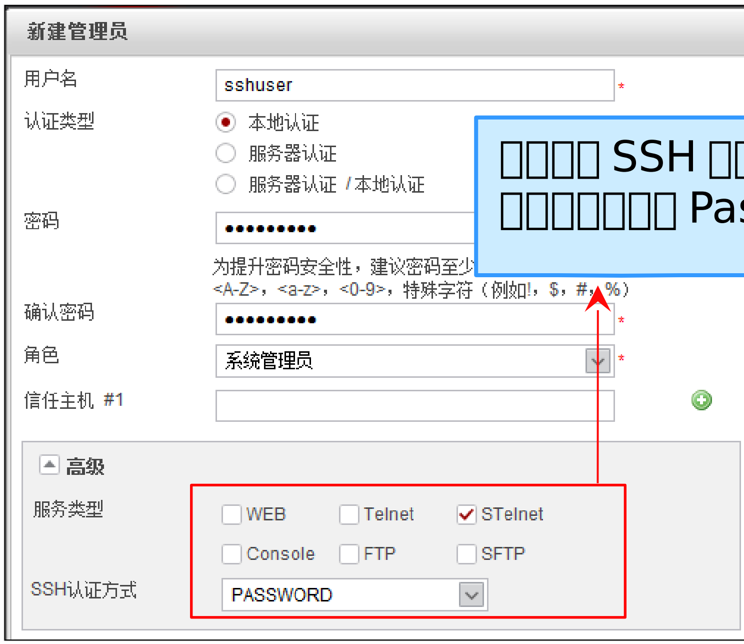
SSH 设备管理类型

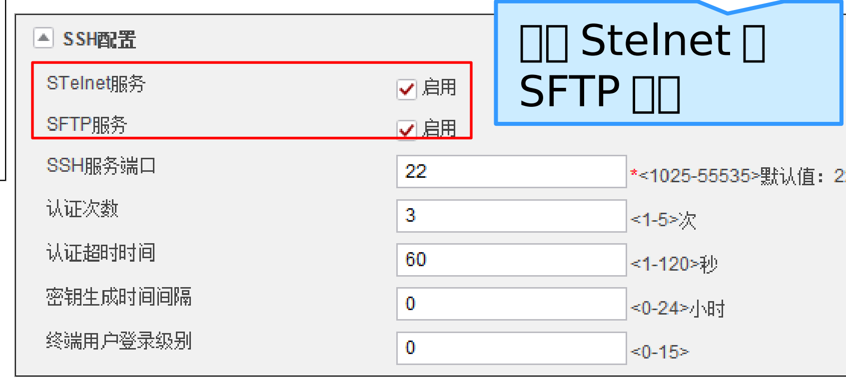
• 创建管理员Client01，并设置设备管理类型为SSH。

必须设置SSH 认证方式
设置认证方式为 Password

• SSH option（Notes: 默认Console, telnet, ftp配置，无需另外配置)

启用Stelnet和
SFTP服务





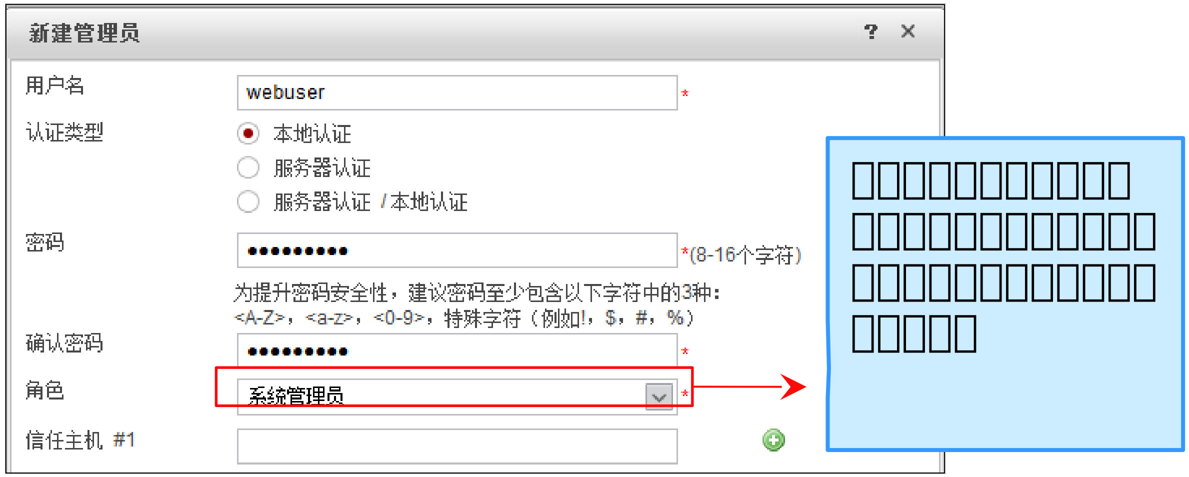
Web设备管理类型

• 创建管理员webuser，设置用户级别。

用户角色设置为系统管理
员，不仅可以配置设备，而
且可以管理文件系统，用于
软件升级。

• 在“系统 > 管理员 > 设置”设置 HTTPS/HTTP服务端口, 当使用 HTTP登录设备后，不可以关闭 HTTP服务，同时不能修改 HTTP服务端口；当使用 HTTPS登录设备后，不可以关闭 HTTPS服务，同时不能修改 HTTPS服务端口。

启用 HTTPS服务，设置
HTTPS服务端口。



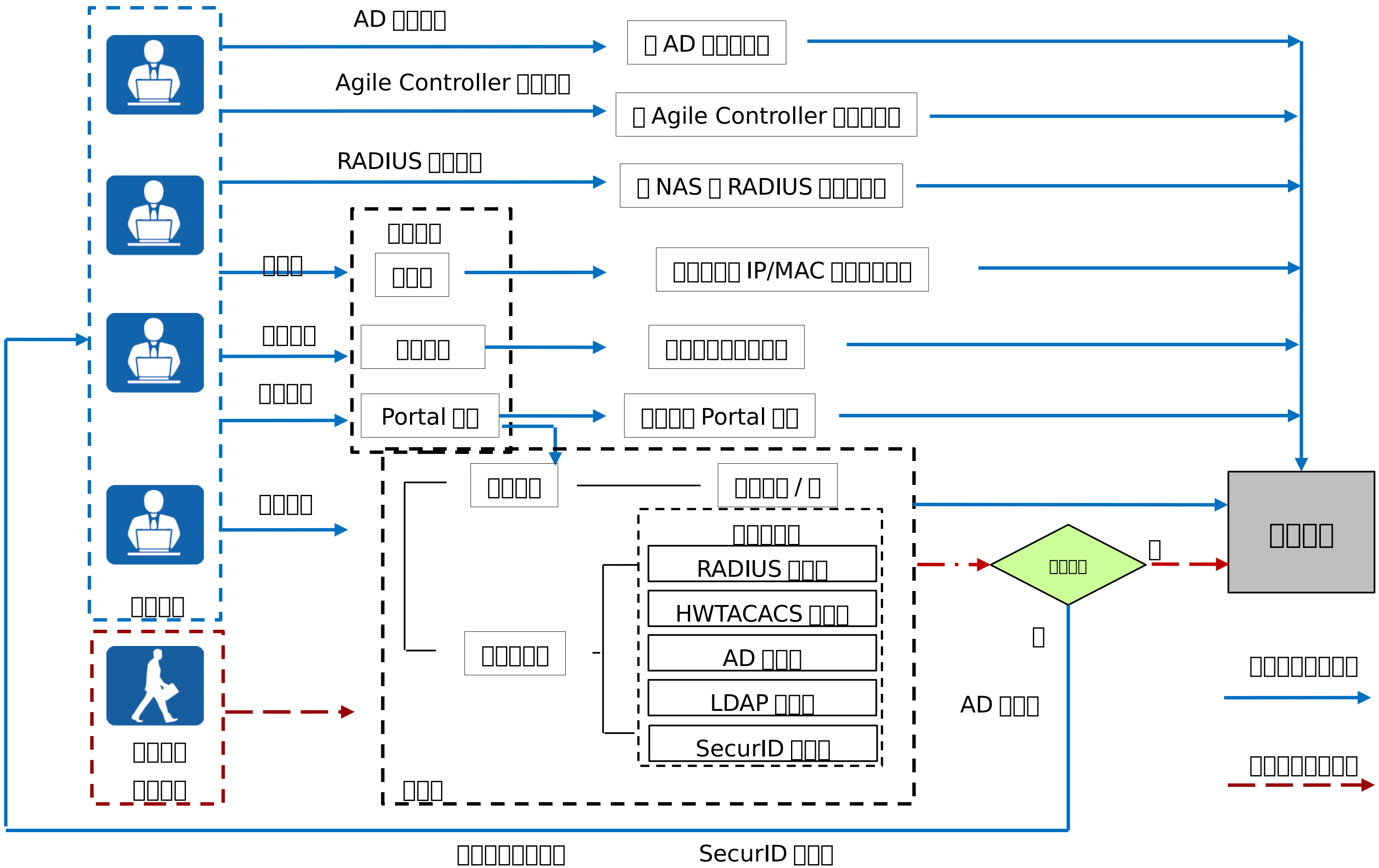
目录

1. 用户认证和 AAA 技术原理

2. 用户认证管理及应用

- 用户组织架构及分类
- 管理员认证流程和配置
- 上网用户及接入用户认证流程
- 用户认证策略
- 上网用户认证配置

□□□□



AD □□□□
□ AD □□□□□
Agile Controller □□□□
□ Agile Controller □□□□□
RADIUS □□□□
□ NAS □ RADIUS □□□□□
□□□□
□□□
□□□
□□□□□ IP/MAC □□□□□□
□□□□
□□□□
□□□□□□□□
□□□□
Portal □□
□□□□ Portal □□
□□□□
□□□□
□□□□ / □
□□□□□
RADIUS □□□
HWTACACS □□□
□□□□□
AD □□□
LDAP □□□
SecurID □□□
□□□
□□□□
□□□□
□
□
AD □□□
□□□□
□□□□
□□□□
□□□□□□□□
□□□□□□□□
□□□□□□□□
SecurID □□□

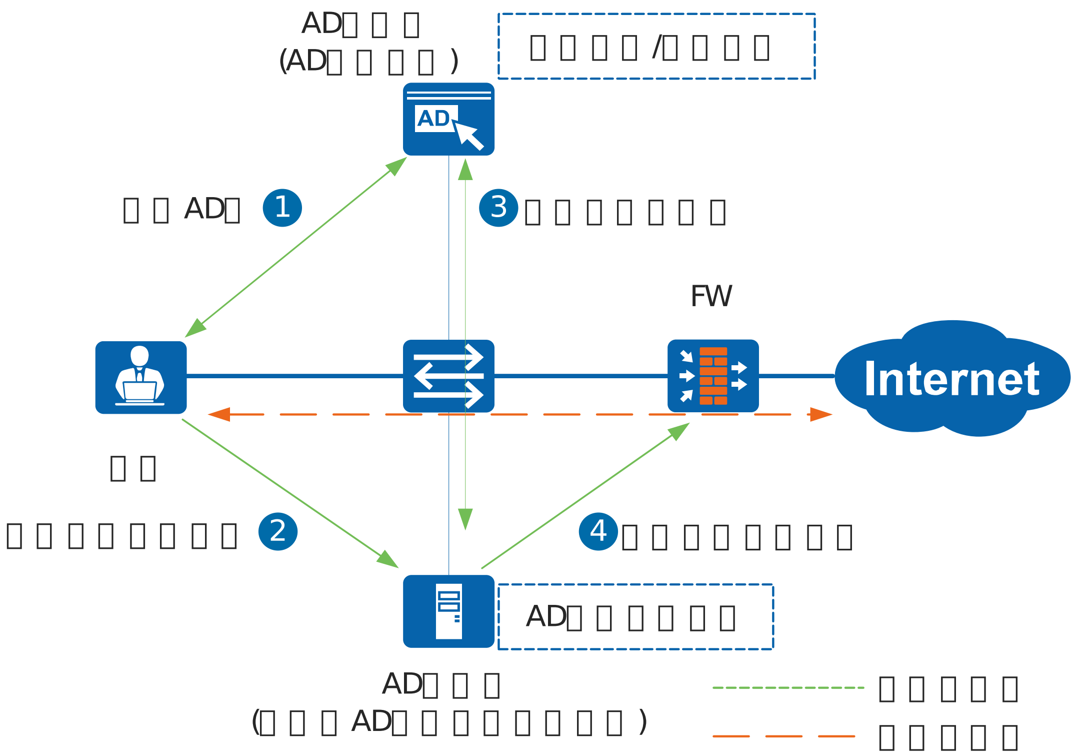
HUAWEI

单点登录

- 单点登录是指防火墙不是认证点，防火墙通过获取其他认证系统的用户登录消息，使用户在防火墙上线。
- AD 单点登录是用户希望经过 AD 服务器的认证后，就会自动通过 FW 的认证，然后可以访问所有的网络资源。 AD 单点登录主要有三种登录实现方式：
  - 接受 PC 消息模式
  - 查询 AD 服务器安全日志模式
  - 防火墙监控 AD 认证报文

AD□□□□（□□PC□□□□）

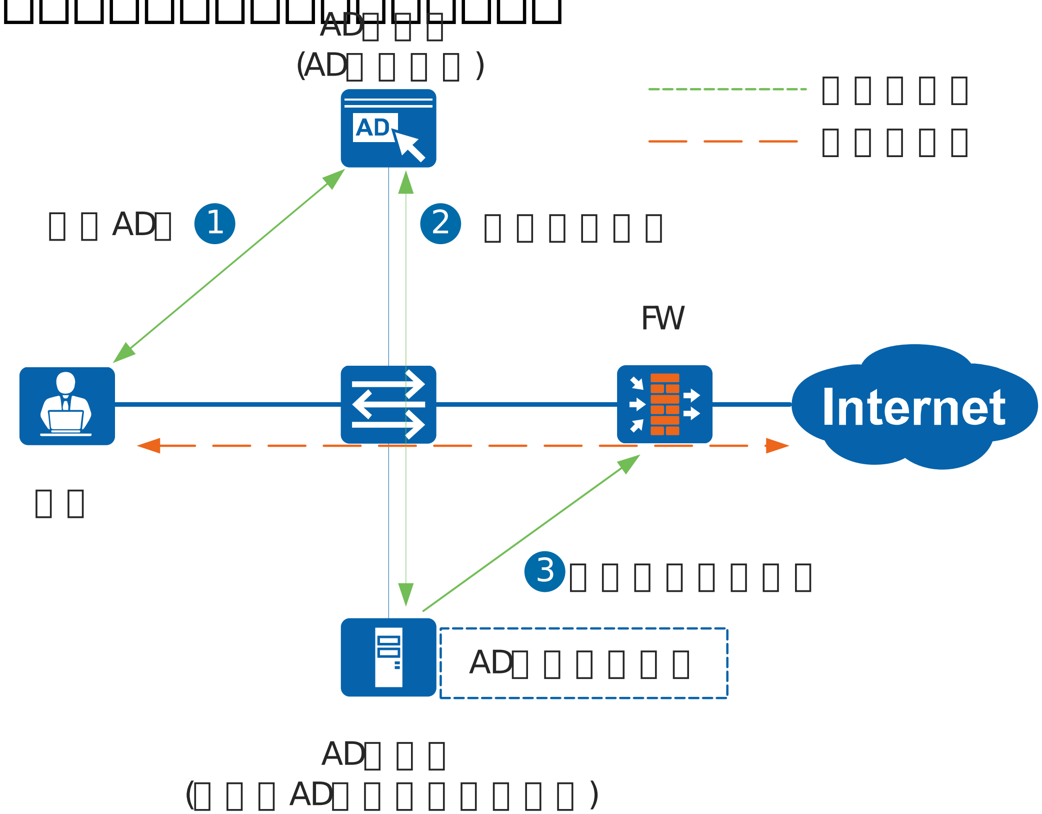
- □□□□□□AD□□□□□□AD□□□□□□□□AD□□□□AD□□□□□□□□□□□□□□□□□
  □□□□□□□□□□AD□□□□□□□□□AD□□□□□□□□□□□□□/□□□□□



□□□□ © 2018 □□□□□□□□

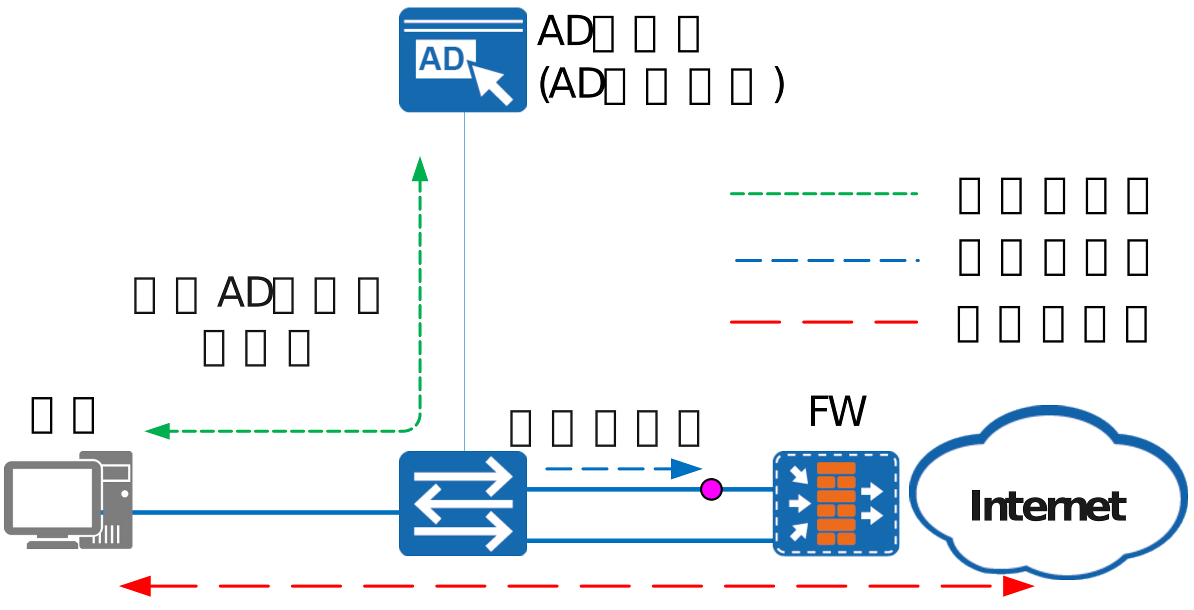
AD □□□□（□□AD □□□□□□□□□）

- □□□□AD □□□□AD □□□□□□□FW □□AD □□□□
  □□AD □□□□□□□□□□□



AD□□□□（□□□□□AD□□□□）

- □□□□□□AD□□□□□□□□□FW□□□□□□□□□AD□□□□□□□□□□□□□□□□□□□□□□□□□IP□□□□□□□□□□□□□□



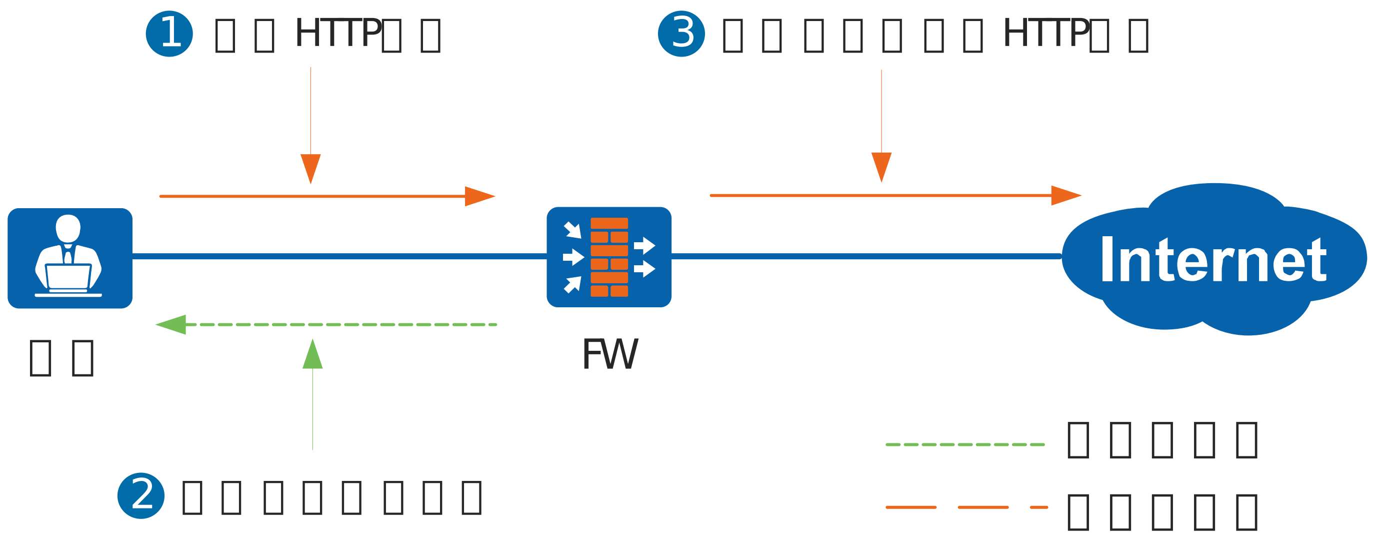
上网用户 Portal 认证

- Portal 认证是指由防火墙或第三方服务器提供 Portal 认证页面对用户进行认证。防火墙内置 Portal 认证的触发方式包括：
  - 会话认证：
    - 会话认证是用户不主动进行身份认证，先进行 HTTP 业务访问，在访问过程中进行认证。认证通过后，再进行业务访问。
  - 事前认证：
    - 事前认证是指访问者在访问网络资源之前，先主动进行身份认证，认证通过后，再访问网络资源。

版权所有 © 2018 华为技术有限公司

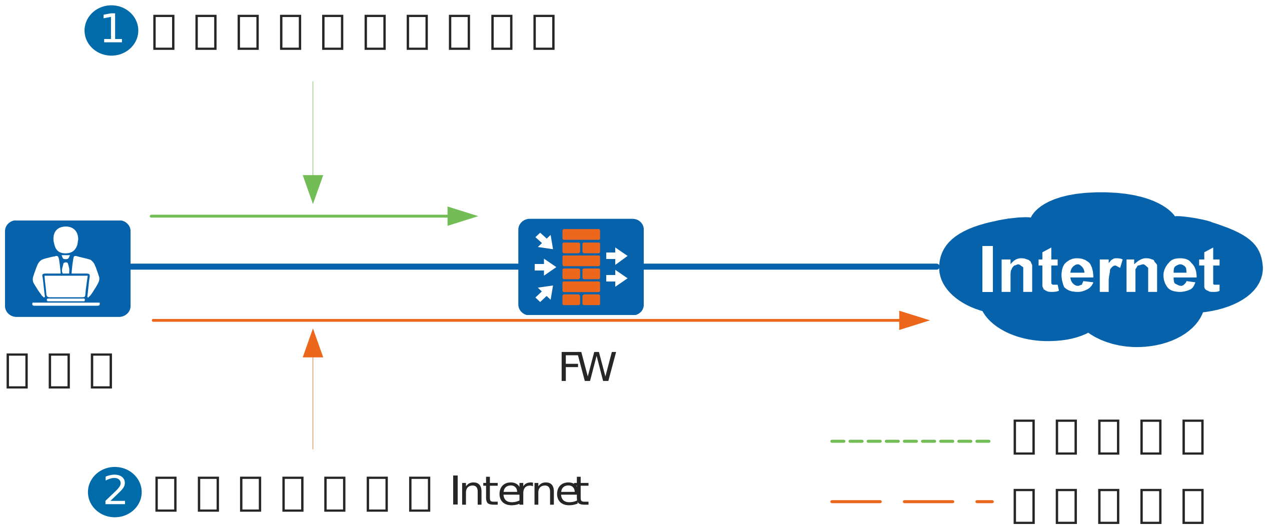
[illegible] Portal [illegible] - [illegible]

- [illegible] HTTP [illegible] HTTP [illegible]
  [illegible] HTTP [illegible]



□□Portal□□□□□□ - □□□□

- □□□□□□□□□□□□□□□□□□□□□□FW□□□□□□□□□□□□□□□□□□□□□□□□□□□Internet□



□□□□ © 2018 □□□□□□□□

接入用户认证

- 接入用户认证指的是对各类 VPN 接入用户进行认证。触发认证的方式由接入方式决定，包括：
  - SSL VPN
  - L2TP VPN
  - IPSec VPN
  - PPPoE

SSL接入用户访问内部资源举例

Firewa
ll

Applicatio
n server

防火墙验证用户账号和密码

账户A的访问资源

账户 B的访问资源
…

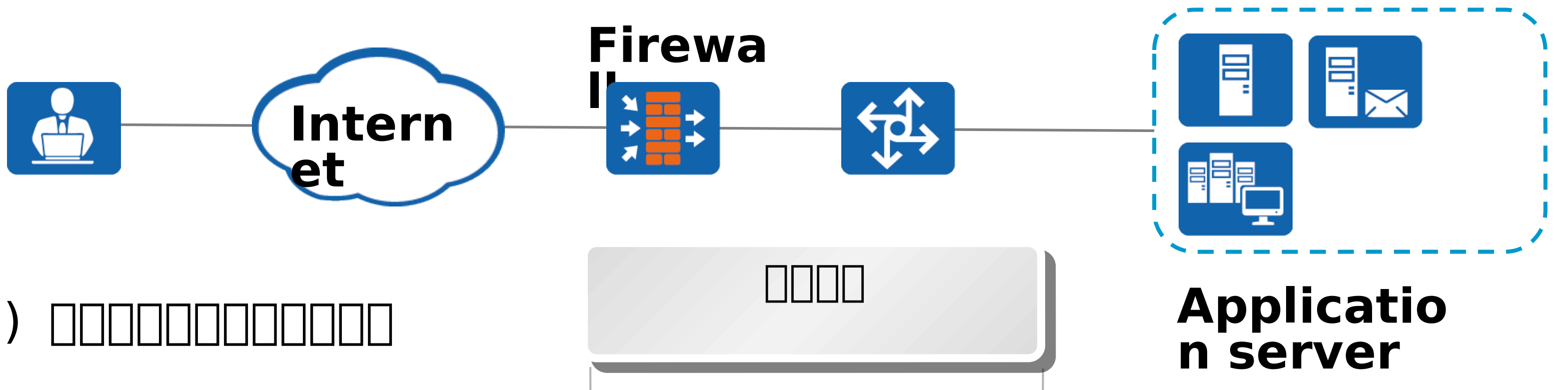
用户账号
(1) 登录设备，提交账户和密码

(2) 通过用户认证

(3) 允许访问

Intern
et

版权所有© 2018 华为技术有限公司 第41页



目录

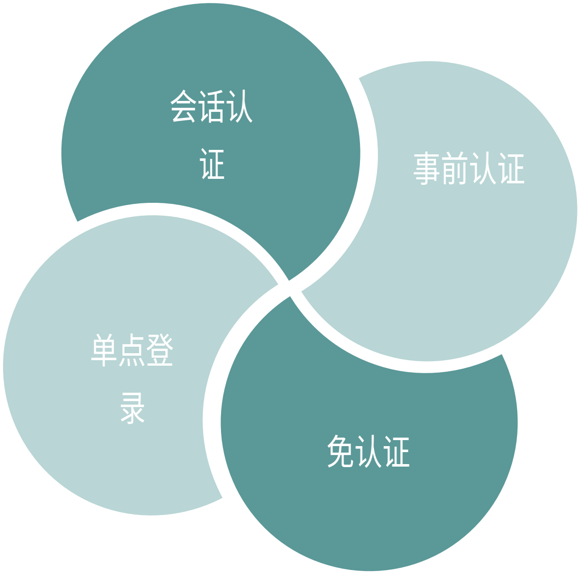
1. 用户认证简介和 AAA 技术原理

2. 用户认证管理及应用
   - 用户组织架构及分类
   - 管理员认证流程和配置
   - 上网用户及接入用户认证流程
   - 用户认证策略
   - 上网用户认证配置

版权所有 © 2018 华为技术有限公司

认证策略

- 认证策略用于决定防火墙需要对哪些数据流进行认证，匹配认证策略的数据流必须经过防火墙的身份认证才能通过。缺省情况下，防火墙不对经过自身的数据流进行认证，需要通过认证策略选出需要进行认证的数据流。如果经过防火墙的流量匹配了认证策略将触发如下动作：



版权所有 © 2018 华为技术有限公司

认证策略组成信息

- 认证策略是多个认证策略规则的集合，认证策略决定是否对一条流量进行认证。认证策略规则由条件和动作组成，条件指的是FW匹配报文的依据，包括：
  - 源/目的安全区域
  - 源地址/地区
  - 目的地址/地区
- 动作指的是FW对匹配到的数据流采取的处理方式，包括：
  - Portal认证
  - 短信认证
  - 免认证
  - 不认证

版权所有 © 2018 华为技术有限公司

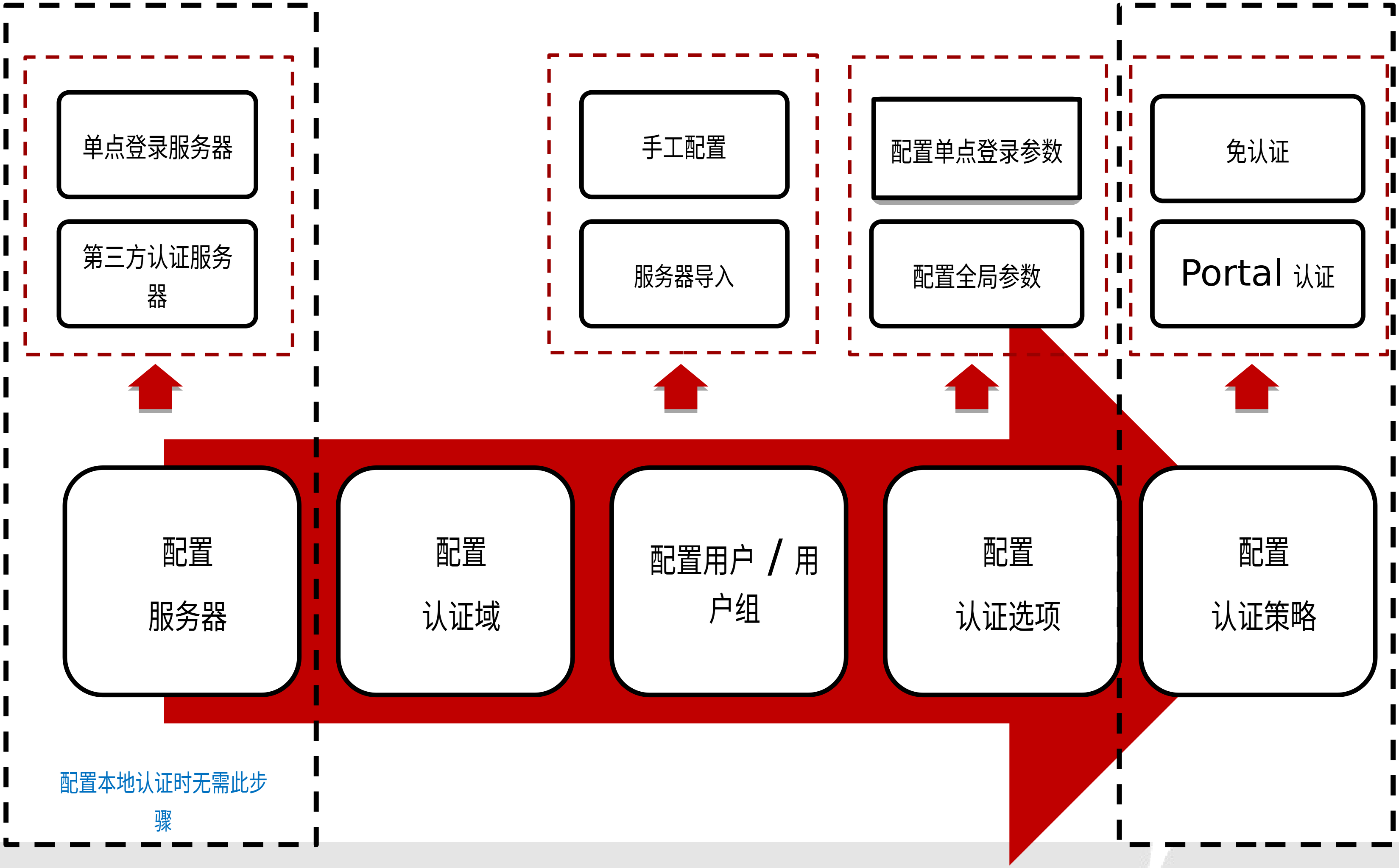
目录

1. 用户认证简介和 AAA 技术原理
2. 用户认证管理及应用
   - 用户组织架构及分类
   - 管理员认证流程和配置
   - 上网用户及接入用户认证流程
   - 用户认证策略
   - 上网用户认证配置

版权所有 © 2018 华为技术有限公司

HUAWEI

配置流程

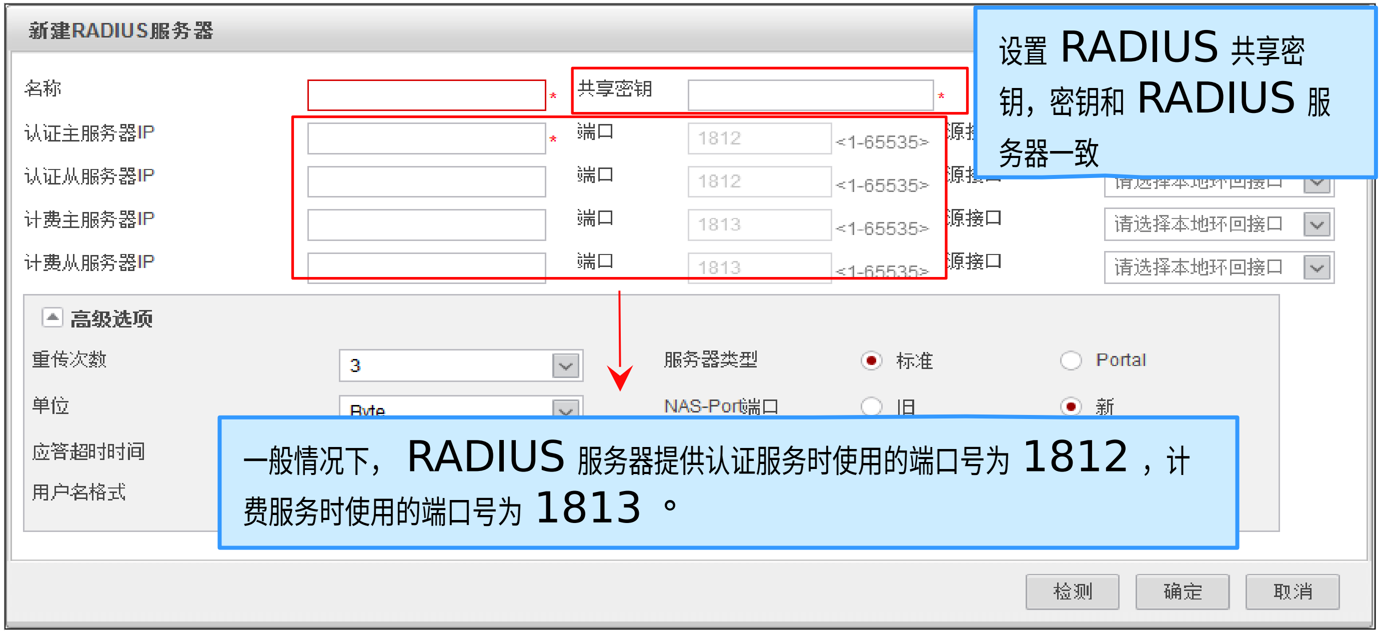


单点登录服务器
第三方认证服务器
手工配置
服务器导入
配置单点登录参数
配置全局参数
免认证
Portal 认证
配置服务器
配置认证域
配置用户 / 用户组
配置认证选项
配置认证策略
配置本地认证时无需此步骤

HUAWEI

配置服务器（RADIUS）

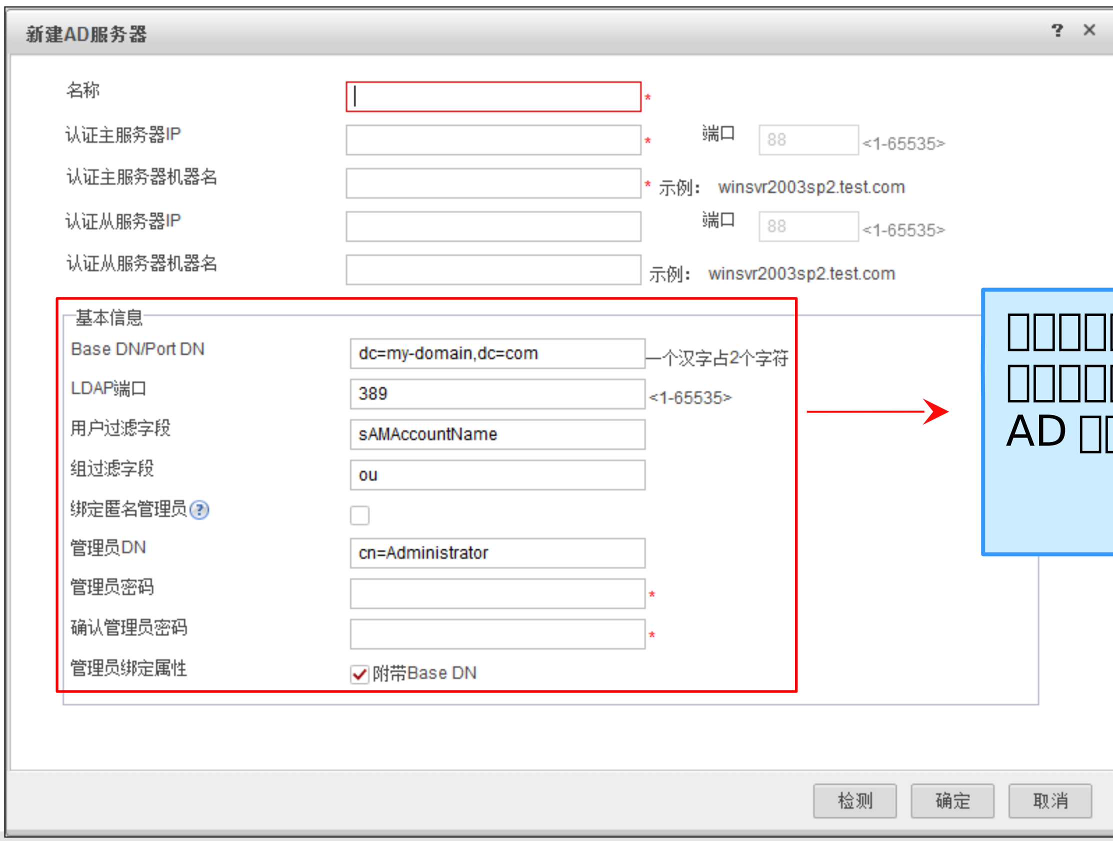
- 在“对象 > 认证服务器 > RADIUS > 新建”，新建 RADIUS 服务器。



版权所有 © 2018 华为技术有限公司

□□□□□（AD)

- □“□□ > □□□□□ > AD > □□”□□□ AD □□□□



新建AD服务器
名称
认证主服务器IP
端口
88
<1-65535>
认证主服务器机器名
示例： winsvr2003sp2.test.com
认证从服务器IP
端口
88
<1-65535>
认证从服务器机器名
示例： winsvr2003sp2.test.com
基本信息
Base DN/Port DN
dc=my-domain,dc=com
一个汉字占2个字符
LDAP端口
389
<1-65535>
用户过滤字段
sAMAccountName
组过滤字段
ou
绑定匿名管理员
管理员DN
cn=Administrator
管理员密码
确认管理员密码
管理员绑定属性
附带Base DN
检测
确定
取消

□□□□□□□□ AD □□□□□□□□□□□□□□□ AD □□□□□□□□

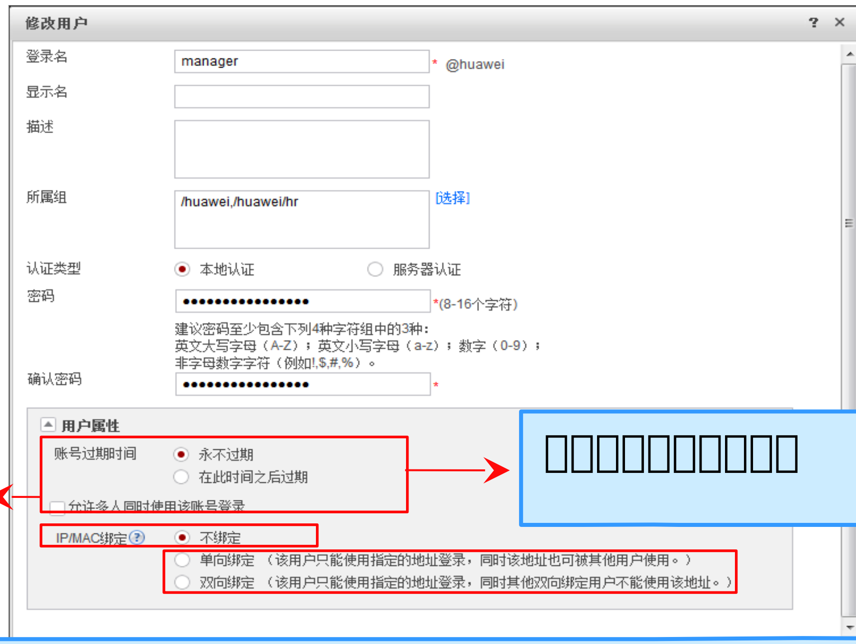
创建用户和用户组

- 在“对象 > 用户 > default ”，新建用户 / 用户组。

表示用户组，列表中只显示该用户组的所属组和描述信息。其他参数均显示为“ --”，即表示非用户组相关参数，不可配置。

表示用户，列表中除能直接显示用户所属组、绑定信息、账号过期时间、描述信息以及当前的用户状态，还能修改用户状态。

版权所有 © 2018 华为技术有限公司


修改用户
登录名
manager
* @huawei
显示名
描述
所属组
/huawei,/huawei/hr
[选择]
认证类型
本地认证
服务器认证
密码
*(8-16个字符)
建议密码至少包含下列4种字符组中的3种：
英文大写字母（A-Z）；英文小写字母（a-z）；数字（0-9）；
非字母数字字符（例如!,$,#,%）。
确认密码
*
用户属性
账号过期时间
永不过期
在此时间之后过期
允许多人同时使用该账号登录
IP/MAC绑定
不绑定
单向绑定 （该用户只能使用指定的地址登录，同时该地址也可被其他用户使用。）
双向绑定 （该用户只能使用指定的地址登录，同时其他双向绑定用户不能使用该地址。）

MAC MAC
MAC

配置认证选项 (全局配置)

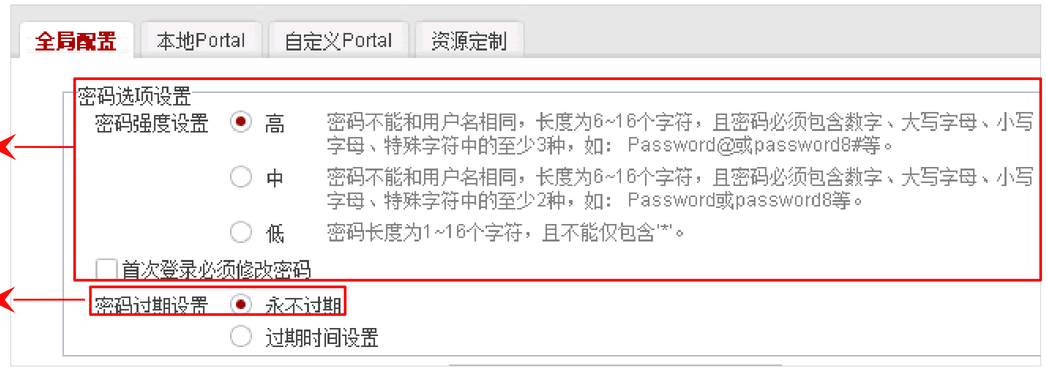
• 在“对象 > 用户 > 认证选项 > 全局配置/本地 Portal”，进行配置。

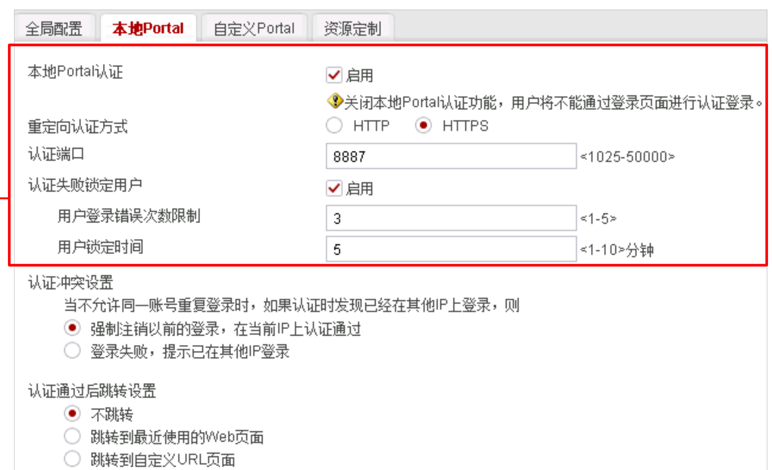
用户可在登录认证页面时对密码
进行修改，且该配置只适用于用
户通过认证页面来修改密码的情
况。

该选项表示用户首次登录认证页
面时，必须修改密码。

上网用户使用web重定向
推送认证页面时需要配置该部
分，认证端口默认使用
8887端口。

版权所有© 2018 华为技术有限公司 第52页





配置认证选项 （ 单点登录 ）

- 在“对象 > 用户 > default > 上网方式及认证策略配置”，配置单点登录。

在上网方式处选择单点登录认证

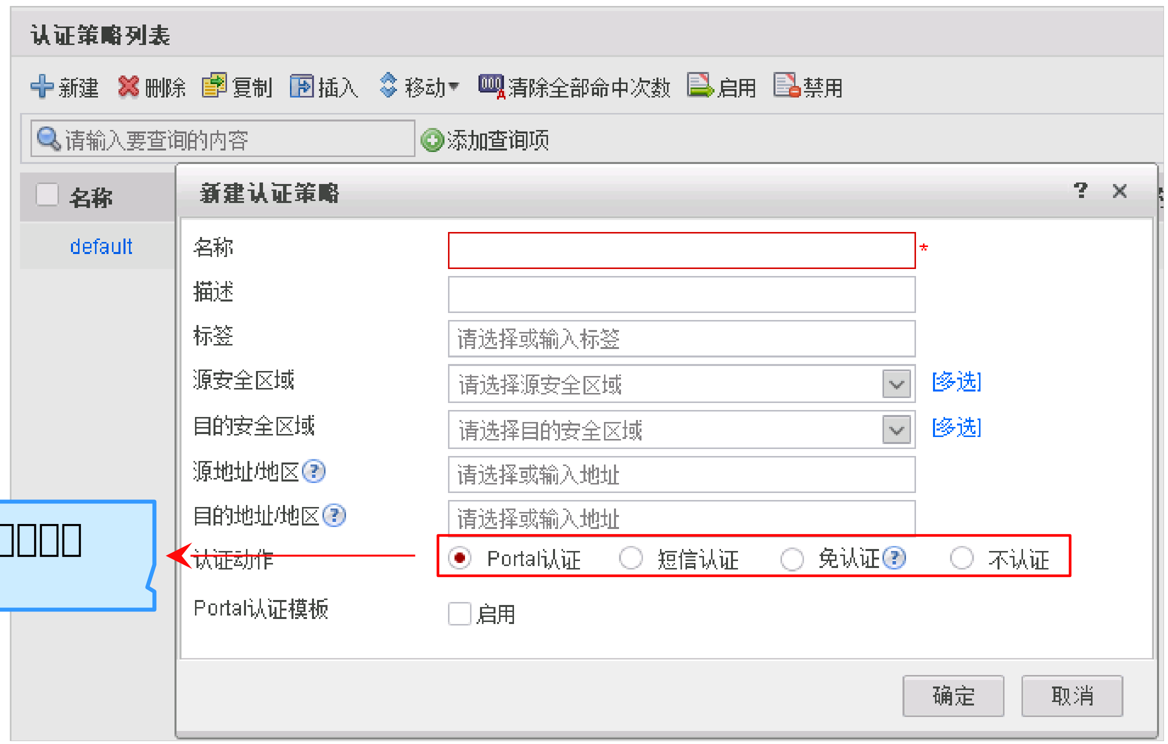
免插件方式的 AD 单点登录。

在使用插件方式配置 AD 单点登录时，需下载 AD 服务器单点登录程序并解压缩。然后在 AD 监控器上安装 ADSSO_Setup.exe，配置 AD 单点登录服务的运行参数。

版权所有 © 2018 华为技术有限公司

[illegible]

- [illegible]“[illegible] > [illegible] > [illegible] > [illegible]”[illegible]

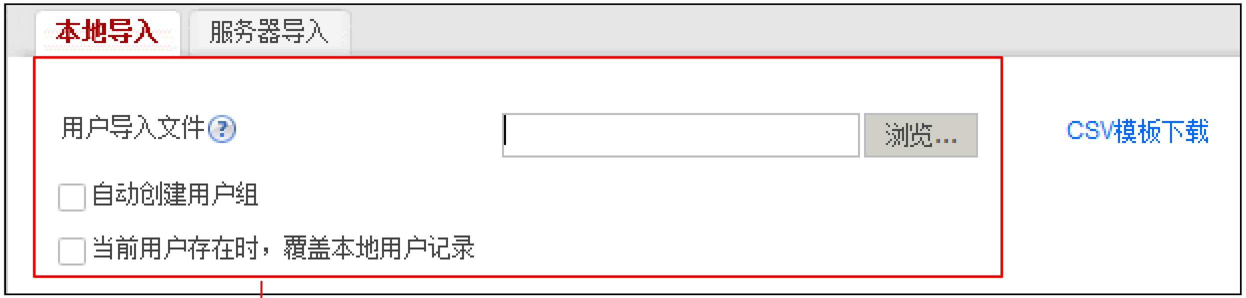


认证策略列表
新建
删除
复制
插入
移动
清除全部命中次数
启用
禁用
请输入要查询的内容
添加查询项
名称
default
新建认证策略
名称
描述
标签
请选择或输入标签
源安全区域
请选择源安全区域
[多选]
目的安全区域
请选择目的安全区域
[多选]
源地址/地区
请选择或输入地址
目的地址/地区
请选择或输入地址
认证动作
Portal认证
短信认证
免认证
不认证
Portal认证模板
启用
确定
取消

[illegible]

通过本地和服务器导入用户

- 选择“对象 ＞ 用户 ＞ 用户导入”。
  - 本地导入：本地导入支持将 CSV 格式文件和数据库 dbm 文件的用户信息导入到设备本地。
  - 服务器导入：从认证服务器上批量导入用户是指通过服务器导入策略，将认证服务器上用户（组）信息导入到设备上。



下载 CSV 模板，补充完整数据后，点击浏览，并上传数据。

版权所有 © 2018 华为技术有限公司

[illegible]

- [illegible]“[illegible] > [illegible] > [illegible]”[illegible]
- [illegible]
- [illegible]

[illegible]

组织结构
查询
default (0)
huawei (0)
research center (0)
hr (0)
mk (0)
在线用户列表
刷新
强制注销
全部强制注销
冻结
解冻
登录名(显示名)
所属组
IP地址
认证方式
接入方式
登录时间/冻结时间

[illegible]

思考题

1. 以下哪个选项不属于AAA（ ）？
A. 认证
B. 授权
C. 计费
D. 管理
2. AD单点登录主要有哪三种登录实现方式（ ）？
A. 接受PC消息模式
B. 查询AD服务器安全日志模式
C. 防火墙监控AD认证报文
D. PC直接登录

版权所有© 2018 华为技术有限公司 第57页

本章总结

• 用户认证简介
• AAA技术原理
• 用户认证管理及应用

版权所有© 2018 华为技术有限公司 第58页

[illegible]

www.huawei.com